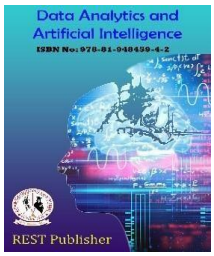
Data Analytics and Artificial Intelligence
Vol: 5(2), 2025
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/daai/
DOI: https://doi.org/10.46632/daai/5/2/4



Enhancing Cybersecurity Through Advanced Cyber Defense and Secure Computing Techniques

Naga Bhuvaneswari Chinnam
Senior Software Engineer, Sam's Club, United States.
Corresponding Author Email: nagabhuvaneswari.chi@gmail.com

Abstract: *Adequate cyber defense and computing are crucial elements for protecting one's digital property from cyber-attacks that are becoming increasingly common. In today's connected world, confidentiality, integrity, and availability are some of the main considerations that need to be addressed. The paper evaluates modern cybersecurity approaches and the importance of cyber defense. The significance of the study can be attributed to the need for adequate ways of handling cybersecurity risks. Cyber defense is very important to protect the confidentiality of organizational data and privacy. The methodology employed in this research is qualitative approach by reviewing available literature on cyber defense and secure computing. From the findings, it can be noted that cyber defense and computing are vital techniques and strategies that ensure adequate security. In conclusion, it is evident that cyber defense and computing are crucial elements in ensuring cybersecurity.*

Keywords: *Cyber Defense, Secure Computing, Cybersecurity.*

1. INTRODUCTION

We have two ways of looking at the defense and security mechanisms of the IoT environment. defense and security mechanisms of the IoT environment, including Intrusion Detection Systems and Intrusion Prevention Systems. How the defense and security systems work in the IoT environment may provide readers with an insight into the latest theoretical and practical developments. The above reviews are informative; nevertheless, they focus on particular themes of the security of the IoT environment, networks, and technologies like blockchain or machine learning. The emergence of the current era of digitalization has brought about many changes as far as the usage of information technologies goes, changing the interactions between both individuals and corporations with these technologies and each other. Digital technologies in activities ranging from online banking to the development of smart cities and using the Internet of Things can now be called indispensable aspects of everyday life. This reliance on digital technologies, in its turn, brings with itself multiple risks of facing cyber-attacks on the part of humans and corporations. For this reason, cyber defense and secure computing have become vital disciplines. Cyber defense can be defined as any action taken to safeguard information systems against any sort of threats originating from cyberspace. Such threats may come in different varieties, for example, malware attacks, ransomware, phishing, denial-of-service, and advanced persistent threats among others. Given the fact that there is always a constant evolution in technology, attackers are always developing new tactics to attack their victims. In order to counter these threats, cyber defense tactics should be flexible enough to include emerging technologies such as artificial intelligence and machine learning as well as behavioral analysis. Cyber defense is all about taking proactive and reactive steps to safeguard the computer networks and systems from any sort of cyber threats. These threats may take many forms and include malicious software, ransomware, phishing attacks, denial of service attacks, and advanced persistent threat activities. Since cyber criminals keep improving their techniques to compromise cybersecurity, it becomes necessary for us to stay on guard and develop our methods of combating them through the use of technologies like artificial intelligence and machine learning. This would ensure that we are better prepared to tackle any kind of cyber-attack before it happens. While secure computing, by contrast, is concerned with developing and designing computing environments which are inherently secure against such security threats. This means that secure computing requires the use of hardware,

Copyright@ REST Publisher

software, and networking systems which take into account security at all stages of computing. Secure computing takes into consideration such factors as secure coding, authentication, access control, and encryption. Moreover, secure computing recognizes the importance of end-users in the field of computer security, since they often become the weakest link in any computer system. CIA stands for confidentiality, integrity, and availability, which are some of the key concepts of cyber defense and secure computing. Confidentiality involves ensuring that sensitive data can be accessed only by those who have been authorized, thus safeguarding such information against any form of unauthorized exposure. On the other hand, integrity involves the assurance that the data will be free from alteration and distortion while in storage or during transmission. Finally, availability is concerned with guaranteeing access to the data or systems at all times. Due to the complexity of the cyber threat landscape, sophisticated methods are being used to protect against attacks. Traditional cybersecurity tools like antivirus and firewalls are no longer enough to provide protection from today's cyber threats. Instead, advanced methods are now being used, including intrusion detection and prevention systems, endpoint protection systems, and the use of a zero-trust architecture. Zero-trust architecture works under the assumption that there is "never trust; always verify," meaning that constant authentication is necessary for the user and device. Threat intelligence is another key element of cybersecurity that refers to the process of collecting and analyzing information on possible cyber threats. Understanding the techniques and methods of work that cybercriminals use allows for more efficient protection from them. Moreover, threat intelligence allows for the development of stronger relationships between different organizations in order to exchange information about possible cyber threats and create better defenses against them. A secure computer also has a crucial place in keeping private data safe, especially within industries like medicine, banking, and governments. Such industries have plenty of data on individuals and are thus more likely to face cyberattacks. One of the best ways of keeping your data safe is encrypting it, ensuring that any intruder who gains access to the information will not be able to decipher it because of lack of a decryption key. Other useful tools in keeping private data safe include multi-factor authentication and biometric verification.

2. MATERIALS AND METHOD

In the current research, the input variables include firewall_log_score, login_attempts, and threat_detected, whereas the output variable includes network_traffic_rate. The firewall log score variable denotes the level of security activity reported in the log file of the computer system. On the other hand, login_attempts denotes the frequency at which people are accessing the computer system. Threat_detected variable refers to whether there was any potential security breach detected. In combination, the above variables provide information regarding activity within the computer system and any possible anomaly. Network_traffic_rate is the output variable because it denotes the amount of data passing through the network.

Support Vector Regression (SVR)

Support Vector Regression (SVR) is a supervised machine learning algorithm used to predict continuous numerical values by identifying an optimal regression function. It is based on the principles of Support Vector Machines (SVM) and aims to minimize prediction errors while maintaining model complexity. SVR uses a margin-based approach in which deviations within a predefined tolerance, known as the epsilon (ε) margin, are not penalized. This approach helps the model achieve better generalization and reduces the influence of small variations in training data. SVR can handle both linear and nonlinear relationships through different kernel functions, including linear, polynomial, radial basis function (RBF), and sigmoid kernels. The optimization process identifies support vectors, which are important observations that determine the position and structure of the regression function. The performance of SVR depends on parameters such as the regularization parameter (C), epsilon (ε), and kernel coefficient (γ). Proper parameter selection improves prediction accuracy and minimizes overfitting. SVR is widely applied in engineering, financial forecasting, energy prediction, materials science, and industrial performance analysis because of its ability to model complex relationships and provide reliable predictions from limited datasets.

Copyright@ REST Publisher

3. RESULT AND DISCUSSION

TABLE 1. Descriptive Statistics

	firewall_log_score	network_traffic_rate	login_attempts	threat_detected
count	250	250	250	250
mean	54.796	1099.248	15.212	0.436
std	27.42925	505.7798	8.581704	0.496882
min	10	201	1	0
25%	31	690.75	7	0
50%	56.5	1107.5	16	0
75%	78.75	1498.75	23	1
max	99	1999	29	1

The above data set represents the data for 250 records of cyber security indicator observations. On an average, the firewall log score is observed to be around 54.8, representing moderate security alert scores, whereas the network traffic value is seen to be close to 1099. Login attempt values are found to be on average 15. For the threat_detected variable, the average score is 0.436, which shows that the threat was detected almost 44 percent of the time.

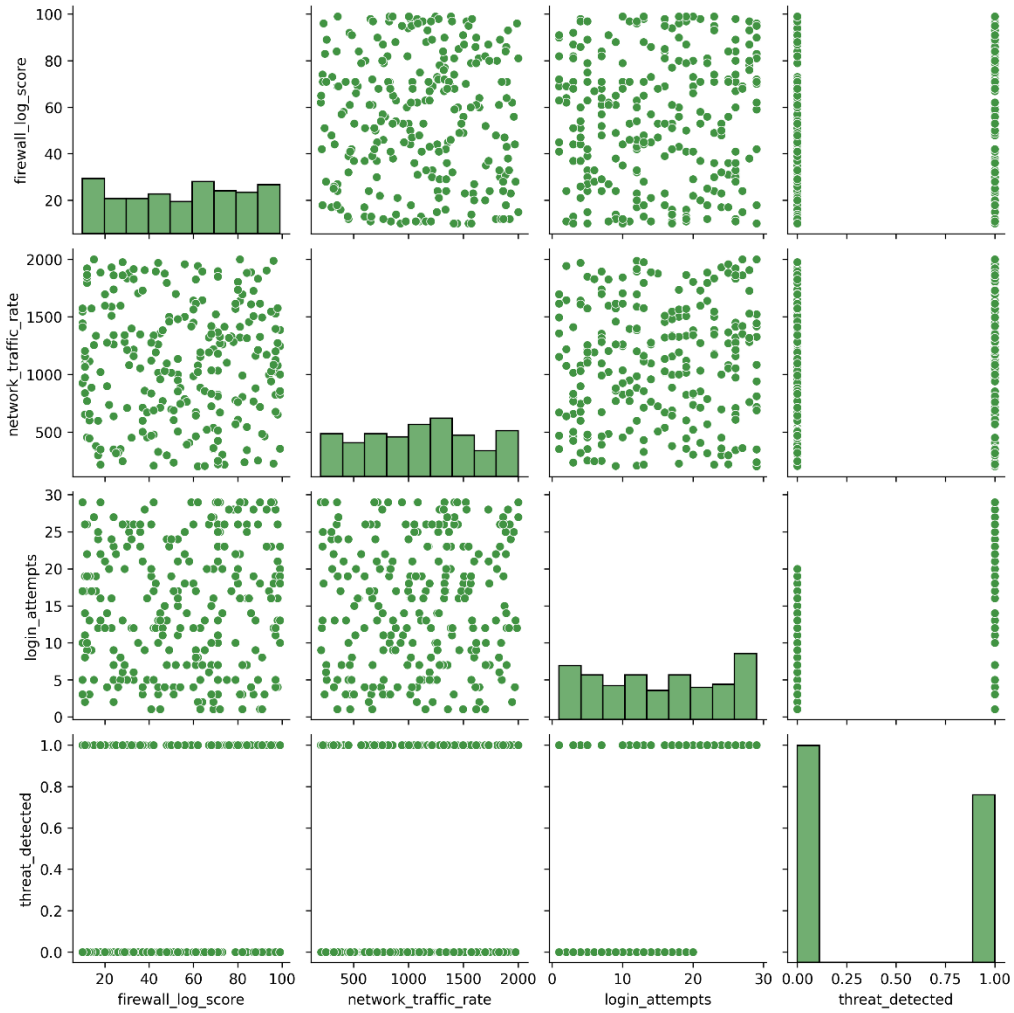


FIGURE 1. Correlation Between Different Cybersecurity Activities

Figure 1 demonstrates the pairplot analysis for the relevant variables in terms of cyberattacks, including the firewall log score, network traffic rate, number of login attempts, and threat detected. From the histograms on the diagonals, it can be concluded that the distribution of the variables under study does not exhibit any significant skewness. As

seen from the scatter plots, there are only weak correlations between most of the studied variables, which indicates that the variables like firewall logs, traffic rate, and login attempts do not have any significant association.

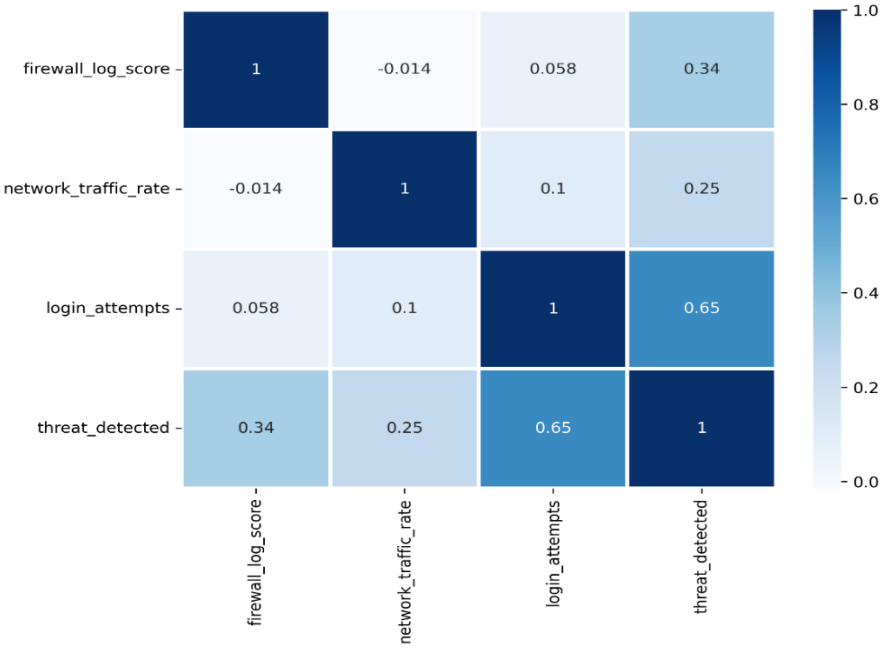


FIGURE 2. Heat Map Correlation for Cyber Security Variables.

The figure below shows the heat map correlation chart for firewall log score, network traffic rate, login attempts, and threat detection. From the heat map correlation shown above, one can note that login attempts possess the highest positive correlation coefficient (0.65) with threat detection; thus, the more the login attempts, the more the threats are detected. Furthermore, there exists a positive correlation of 0.34 between firewall log score and threat detection, which implies that attacks can happen as a result of high firewall logs. It is worth noting that the amount of multicollinearity is minimal, since the correlation coefficients among the independent variables are low.

Support Vector Regression

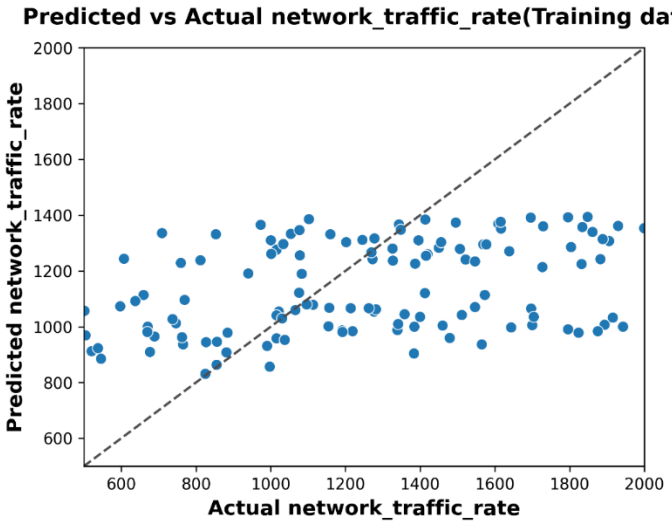


FIGURE 3. Actual vs. Predicted Values of Network Traffic Rate (Training Data Set)

Copyright@ REST Publisher

The scatter plot shown in Figure 3 compares the actual and predicted values for network traffic rate based on the training data set. As seen in the figure, the dotted line shows the ideal line of best fit, which would mean no error in predicting the outcome. Although some points fall close to the dotted line, there are many points deviated from it, thus showing prediction errors. Most of the points in the scatter plot are grouped closely along one end of the graph, showing under-fitting where the model failed to capture the variations in actual traffic rate.

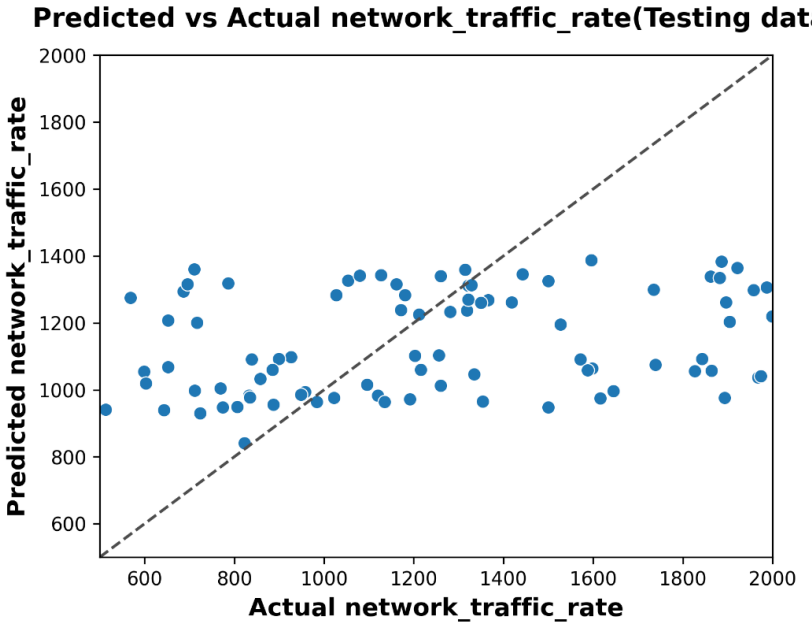


FIGURE 4. Predicted vs Actual Network Traffic Rate (Testing Dataset)

As seen in Figure 4, the discrepancy between the actual and predicted network traffic rates on the testing dataset is represented. The dashed diagonal line represents an optimal prediction, meaning that the prediction matches the actual data point perfectly. However, as seen in the figure, there is still a substantial spread around the line, indicating prediction error. As was the case with the training dataset, there are many predicted data points that fall within a specific narrow range. It can also be observed that there are deviations in predictions, particularly for high and low values.

TABLE 2. Model Performance Comparison on Training Dataset

Data	Symbol	R2	EVS	MSE	RMSE	MAE	Max Error	MSLE	Med AE
Train	SVR	0.100727	0.106898	228947.5	478.4846	390.553	1066.711	0.364426	331.1919

The results of the SVR model's performance measures based on the training data set show a rather low level of accuracy of the algorithm's predictions. The R^2 coefficient (0.1007) and EVS (0.1069) prove that only 10 percent of the variance in traffic rate can be explained by the algorithm, which means that it is a case of weak pattern identification. Furthermore, the values of MSE (228,947.5) and RMSE (478.48) point out a significant amount of prediction errors, while MAE (227.1) shows that the average forecast error does not exceed 227 units. However, a deviation above 1000 also proves a large amount of inconsistency.

TABLE 3. Model Performance Comparison on Testing Dataset

Data	Symbol	R2	EVS	MSE	RMSE	MAE	Max Error	MSLE	Med AE
Test	SVR	0.058583	0.061293	239967.3	489.8646	397.1153	1057.112	0.309101	360.0247

This is evident from the performance measures of the SVR technique when assessing the predictive accuracy of the algorithm based on the testing data. The low values of the R^2 (0.0586) and EVS (0.0613) indicate the low predictive and generalization abilities of the regression model, respectively, explaining about 6% of the variability of the network

Copyright@ REST Publisher

traffic rate. A high value of MSE (239,967.3) and RMSE (489.86) suggests large errors in prediction, whereas MAE (397.12) indicates high deviation of predictions from the actual value, while maximum error of more than 1000 signifies large errors in some cases.

4. CONCLUSION

In the last assessment of the cybersecurity data and SVR models, although clear trends exist in the data set, the predictive ability of the SVR model is insufficient. Based on exploratory analysis tools like pair plots and correlation matrix, it was observed that logins are strongly correlated with cyber threat detection, while other variables are moderately correlated. However, based on the predictive modeling process, various issues arise. Firstly, the behavior of the training and testing metrics is defined by their low R^2 and error values, which show that the SVR algorithm cannot be used for modeling the data set trends. Second, the consistency between the training and testing errors implies an underfitting problem rather than overfitting. Third, the plots showing the difference between the predicted and actual outputs illustrate that the SVR model cannot produce accurate predictions.

REFERENCES

[1]. Szymoniak, Sabina, Jacek Piątkowski, and Mirosław Kurkowski. "Defense and security mechanisms in the internet of things: A review." Applied Sciences 15, no. 2 (2025): 499.

[2]. Zhukabayeva, Tamara, Lazzat Zholshiyeva, Nurdaulet Karabayev, Shafiullah Khan, and Noha Alnazzawi. "Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions." Sensors 25, no. 1 (2025): 213.

[3]. Alzahrani, Taher, and Waeal J. Obidallah. "Adaptive Cyber Defense for Renewable Energy Systems Using Digital Forensics and Fuzzy Multi-Criteria Analysis." Sustainability 18, no. 3 (2026): 1334.

[4]. Ahmad, Waqas, Aamir Rasool, Abdul Rehman Javed, Thar Baker, and Zunera Jalil. "Cyber security in iot-based cloud computing: A comprehensive survey." Electronics 11, no. 1 (2021): 16.

[5]. Thapa, Niraj, Zhipeng Liu, Addison Shaver, Albert Esterline, Balakrishna Gokaraju, and Kaushik Roy. "Secure cyber defense: An analysis of network intrusion-based dataset CCD-IDSv1 with machine learning and deep learning models." Electronics 10, no. 15 (2021): 1747.

[6]. Zhukabayeva, Tamara, Zulfiqar Ahmad, Aigul Adamova, Nurdaulet Karabayev, and Assel Abdildayeva. "An edge-computing-based integrated framework for network traffic analysis and intrusion detection to enhance cyber–physical system security in industrial iot." Sensors 25, no. 8 (2025): 2395.

[7]. Alotaibi, Bandar. "A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities." Sensors 23, no. 17 (2023): 7470.

[8]. Steingartner, William, Darko Galinec, and Andrija Kozina. "Threat defense: Cyber deception approach and education for resilience in hybrid threats model." Symmetry 13, no. 4 (2021): 597.

[9]. Aldhyani, Theyazn HH, and Hasan Alkahtani. "Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model." Mathematics 11, no. 1 (2023): 233.

[10]. Reyes-Acosta, Ricardo Emmanuel, Ricardo Mendoza-González, Edgar Oswaldo Diaz, Miguel Vargas Martin, Francisco Javier Luna Rosas, Julio César Martínez Romo, and Alfredo Mendoza-González. "Cybersecurity conceptual framework applied to edge computing and internet of things environments." Electronics 14, no. 11 (2025): 2109.

[11]. Sebestyen, Hannelore, Daniela Elena Popescu, and Rodica Doina Zmaranda. "A literature review on security in the Internet of Things: Identifying and analysing critical categories." Computers 14, no. 2 (2025): 61.

[12]. Sun, Xiaoqiang, F. Richard Yu, Peng Zhang, Weixin Xie, and Xiang Peng. "A survey on secure computation based on homomorphic encryption in vehicular ad hoc networks." Sensors 20, no. 15 (2020): 4253.

[13]. Tran, Minh-Quang, Mahmoud Elsisi, Meng-Kun Liu, Viet Q. Vu, Karar Mahmoud, Mohamed MF Darwish, Almoataz Y. Abdelaziz, and Matti Lehtonen. "Reliable deep learning and IoT-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification." IEEE Access 10 (2022): 23186-23197.

[14]. Liu, Yingze, and Yuanbo Guo. "Towards real-time warning and defense strategy AI planning for cyber security systems aided by security ontology." Electronics 11, no. 24 (2022): 4128.

[15]. Sarker, Iqbal H., Yoosef B. Abushark, Fawaz Alsolami, and Asif Irshad Khan. "Intrudtree: a machine learning based cyber security intrusion detection model." Symmetry 12, no. 5 (2020): 754.

[16]. Drucker, H., Burges, C. J. C., Kaufman, L., Smola, A., & Vapnik, V. (1997). Support vector regression machines. Advances in Neural Information Processing Systems, 9, 155–161.

[17]. Vapnik, V. N. (1995). The Nature of Statistical Learning Theory. Springer, New York.

[18]. Smola, A. J., & Schölkopf, B. (2004). A tutorial on support vector regression. Statistics and Computing, 14, 199–222.

[19]. Schölkopf, B., & Smola, A. J. (2002). Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond. MIT Press.

[20]. Basak, D., Pal, S., & Patranabis, D. C. (2007). Support vector regression. Neural Information Processing–Letters and Reviews, 11(10), 203–224.

Copyright@ REST Publisher